

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Terry Hedrick, a Special Agent with the United States Secret Service (USSS) being first duly sworn, hereby depose and state as follows:

AFFIANT'S BACKGROUND AND EXPERIENCE

1. I am a Special Agent with the United States Secret Service (hereinafter, the "USSS"), Charleston, WV Resident Office, and have been so employed since December of 2004. I am authorized, pursuant to 18 U.S.C. § 3056(b), to detect and arrest any person who violates any of the laws of the United States relating to electronic fund transfer frauds, access device frauds, false identification documents or devices, and any fraud or criminal or unlawful activity or against any federally insured financial institution. Additionally, I am authorized, pursuant to 18 U.S.C. § 3056(c), to execute warrants issued under the laws of the United States.

2. Since becoming a Secret Service Special Agent, I have personally investigated and/or assisted in investigations relating to violations of the laws of the United States relating to financial crimes, including romance frauds and other online schemes, specifically 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. §§ 1956-57 (money laundering) and 18 U.S.C. 2315 (receipt of stolen property). I received 30 weeks of training at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, and Secret Service's Rowley Training Center in Beltsville, Maryland, before my assignment as a Secret Service Special Agent in the Charleston, WV Resident Office.

3. As a Special Agent with the USSS, I have been involved in other financial elder abuse and romance fraud investigations. I know from my training and experience that those persons involved in committing those types of crimes spend a great deal of time each week seeking out potential victims through email, text messages, social media websites such as Google

Hangouts, Go Fish, Plenty of Fish and various dating sites. I also know that people who commit these crimes stay in constant contact with victims, creating a friendship that ultimately leads to a false romantic relationship with victims. I know that these fraudsters tell their victims untrue stories about their employment, their personal life, their family life and their need for financial assistance. In many of these instances, the fraudsters propose marriage to the victim. I know that after this romance flourishes, the fraudsters then ask victims to send them money for various reasons. Some of the fraudsters' reasons include family medical emergencies, or because the fraudsters need to pay their oil rig workers, or need money to ship gold or other valuables back to the United States to be allegedly shared with the victims or finally, for bail when the fraudsters were allegedly arrested after leaving a foreign country.

4. I know from my training and experience that these fraudsters instruct their victims to send large amounts of currency through the U.S. Mail, FedEx and through the United Parcel Service (UPS). I know that these fraudsters get their victims to send money to them via cashier checks, personal checks, money orders, wire transfers, bitcoin and through many different mobile payment processing companies. These mobile payment processing companies include Transferwise, Ping Express, Money Gram, Western Union, Walmart, Pay Pal, Square, Cash App, Xoom, Zelle, and others.

5. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents, investigators and witnesses. This Affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this Affidavit is taken from financial records, interviews with witnesses, and information shared with me from other investigators and state officials. This ongoing investigation is financial in nature,

thus, any figures I cite in this Affidavit are based on calculations and tracing conducted to date and may be subject to revision at a later date.

6. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1341, 1343, 1957 and 2315 have been committed by Augustine C Chukwu Noe AMECHI, also known as Augustine A Chukwu Noe and Augustine Amechi Chukwu Noe (“AMECHI”).

PURPOSE OF THIS AFFIDAVIT

7. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including those properties and/or persons listed below (collectively the “SUBJECT PREMISES”) for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity); and 18 U.S.C. § 2315 (receipt of Stolen Property), which items are more specifically described in Attachment B of this Affidavit. This Affidavit is also being submitted in support of an application under Rule 41 of the Federal Rules Criminal Procedure for a search warrant for the SUBJECT PREMISES in order to effectuate the arrest of AMECHI.

a. AMECHI

i. The person of AMECHI

ii. The entire property located 1826 7th Avenue, Apartment 2, Huntington, WV 25703;

1. 1826 7th Avenue, Apartment 2, Huntington, WV 25703 is believed to be AMECHI’s primary residence. The

SUBJECT PREMISES is listed as AMECHI's residence on his driver's license and investigators have observed AMECHI at the residence as recently as May 24, 2021.

2. Financial Records obtained during the investigation show that AMECHI has lived at the SUBJECT PREMISES since at least January of 2019, meaning that AMECHI is believed to have resided at the SUBJECT PREMISES during the fraud scheme.

- iii. the content of computers and electronic storage devices located and seized therein; and
- iv. the content of any locked cabinets, containers, drawers, boxes or other receptacles large enough for paper record retention or electronic storage devices located therein.

8. This Affidavit is also submitted in support of an application for a search warrant for the person described in Attachment A of this Affidavit, AMECHI. As set forth herein, there is probable cause to search the person of AMECHI as described in Attachment A, for the items described in Attachment B, including cell phones and digital storage devices such as thumb drives that can be concealed on their person should AMECHI be present in the SUBJECT PREMISES. I believe probable cause exists for the issuance of a warrant to search AMECHI as described in Attachment A, for (1) property that constitutes evidence of a federal criminal offense; (2) contraband, the fruits of a federal crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means for committing a federal criminal offense, namely 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud);

18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity); and 18 U.S.C. § 2315 (receipt of stolen property) (collectively, the “Target Offenses”).

9. From my background and experience, I know that individuals normally maintain records of their financial activity, such as receipts for expenditures by cash and check, bank records, tax returns, escrow files, and other financial documents, in their personal residences and places of business. I am also aware that individuals engaged in illegal activity often possess computers, documents, storage devices, and electronic media used in the commission of the crime and, as set forth below, AMECHI has been known to use computers and other electronic devices. Upon information and belief, most individuals keep their computers and other personal electronic devices at home. Moreover, in my training and experience, people take their computers and other electronic devices when they move to a new location.

10. There are many reasons why individuals, including criminal offenders, maintain evidence for long periods of time. The evidence may be necessary financial records which must be kept for information reporting purposes, such as for state and Federal tax returns, and loan applications. The evidence may also appear innocuous at first glance (e.g., credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes and photographs of vacations or other residences, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but may have real significance and relevance when considered in light of other evidence. The individual at issue may no longer realize they still possess the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The individual may also be under the mistaken belief that they have deleted, hidden, or further

destroyed any computer-related evidence, but which may actually be retrievable by a trained forensic computer expert as detailed later in this Affidavit.

11. Through my training and experience, I am aware that the proceeds generated from both legal and illegal activities may be spent many years after the illegal activity has ceased. Thus, records reflecting income and expenditures for the time spanning the scheme and associated activity and those years immediately following the end of such activity are also essential to any financial investigation.

12. The statements in this Affidavit are based in part on information provided by other investigators, law enforcement officers, witnesses, records obtained through investigation, as well as training and experience and my own investigation of this matter. This ongoing investigation is financial in nature, thus, any figures I cite in this Affidavit are based on calculations and tracing conducted to date and may be revised later. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations or attempted violations of the Target Offenses are presently located in the SUBJECT PREMISES.

STATUTORY AUTHORITY

13. As noted above, this investigation concerns alleged violations of the following:
- a. **18 U.S.C. § 1341** prohibits the use of the postal service or commercial interstate carrier to carry out a scheme to defraud.
 - b. **18 U.S.C. § 1343** prohibits the use of wire, radio, or television communication in interstate or foreign commerce to carry out a scheme to defraud.
 - c. **18 U.S.C. § 1956** prohibits conducting a financial transaction with proceeds

from a specified unlawful activity to promote the unlawful activity or conceal its proceeds.

- d. **18 U.S.C. § 1957** prohibits money transactions involving criminally derived proceeds of a value greater than \$10,000.
- e. **18 U.S.C. § 2315** prohibits the sale or receipt of stolen goods or money more than \$5,000 that has crossed interstate lines.

DEFINITIONS

- 14. The following definitions apply to this Affidavit and Attachment B:
 - a. **“Online schemes”** targeted persons looking for romantic partners, friendship, and other close personal and business relationships on dating websites and other social media platforms. The perpetrators of the schemes created profiles using fictitious and fake names, locations, images, and personas, allowing the perpetrators of the schemes to cultivate relationships with prospective victims. The victims provided money and gifts to the perpetrators of the schemes and were typically asked to conduct transactions on behalf of the perpetrators of the scheme.
 - b. **“Cryptocurrency”** was a form of non-fiat based digital currency, in which transactions are verified and records maintained by a decentralized system using computer data and codes, rather than by a centralized authority. Bitcoin was a type of cryptocurrency.
 - c. **“Zelle”** was a digital payment network and part of a private financial services company owned by Bank of America, BB&T, Capital One, Chase, PNC Bank, U.S. Bank and Wells Fargo. Zelle allowed an individual to electronically

transfer money from his or her bank account to another registered user's bank account, held within the United States, by using a mobile device or the website of a participating banking institution.

- d. "**Computer**," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).
- e. "**Computer hardware**," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- f. "**Computer passwords**" and "**data security devices**," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of

hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, and reverse the process to restore it.

- g. “**Mobile applications**,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, accessing banking information, and transferring monetary funds. Mobile applications are also referred to as “apps” throughout this Affidavit.
- h. A “**Website**” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- i. A “**storage medium**” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.
- j. The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings,

paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact disks, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE TO SEARCH THE PROPERTY DESCRIBED IN ATTACHMENT A AND TO SEIZE THE PROPERTY DESCRIBED IN ATTACHMENT B

15. On April 28, 2021, AMECHI was indicted in the Southern District of West Virginia on charges of wire fraud, money laundering (specifically, unlawful monetary transactions in violation of 18 U.S.C. § 1957), and receipt of stolen property. *See* 3:21-cr-00069. The allegations in the Indictment stemmed from many of the incidents described in the Victim Information Section below. The Indictment is still sealed and not known to AMECHI.

16. AMECHI is associated with Kenneth Emeni (“Emeni”), John Nassy (“Nassy”), Kenneth Ogudu (“Ogudu”), and Oluwabamishe Awolesi also known as Oluwabamise Johnson (“Awolesi”) who were also indicted on fraud rcharges in the Southern District of West Virginia (these individuals and AMECHI are collectively referred to as the “Targets.”). *See* 3:21-cr-00068.

17. Since approximately October 2019, the USSS has been investigating the Targets' actions in early 2016 through at least October 2020, when they conspired to carry out various romance scam frauds and other online scams. As part of the scheme, the Targets and their associates selected and contacted victims through email, text, or online dating and social media websites. The Targets and their associates lulled the victims into believing the victim was in a romantic relationship, friendship, or business relationship with a person using a false and fraudulent identity created by the Targets or their associates. The Targets or their associates then defrauded the victims into sending money to people that the victims believed were their romantic interests, friends, or business associates, when in fact the victims actually sent money to accounts controlled by the Targets.

18. During the investigation, over thirty individuals were interviewed who transferred money to the Targets' bank accounts and multiple victims transferred money to the AMECHI's bank accounts. Some of the information investigators learned from these victims and reviewing their financial records is described in the Victim Information Section below.

19. Many of the victims interviewed informed investigators that they believed that they were in an online relationship and transferred money or items for the benefit of their romantic interests. Other victims were defrauded by cryptocurrency scams, where the Targets or their associates would persuade the victims to wire funds to the Targets to purchase Bitcoin. The victims would send money to purchase Bitcoin but, never received their cryptocurrency. One similarity uniting all of the victims discussed in the Indictment and below is that all of the victims transferred the money to AMECHI upon the requests of the online fraudsters, even though the victims themselves did not know or ever previously meet or communicated with AMECHI.

20. Records obtained during the investigation show that AMECHI has lived at the

SUBJECT PREMISES since at least January of 2019. Specifically, the fraud scheme ran from at least early 2017 through at least May 27, 2020 and AMECHI resided at the SUBJECT PREMISES since January 2019. Investigators believe AMECHI still resides at the SUBJECT PREMISES as he was observed at the SUBJECT PREMISES on May 24, 2021. This means that AMECHI resided at the SUBJECT PREMISES for over a year of the fraud scheme.

21. Moreover, as described in Paragraph 52, a number of suspicious packages were mailed to the SUBJECT PREMISES in 2019 and 2020, when AMECHI resided there.

22. These packages are considered suspicious because they were mailed to the SUBJECT PREMISES but were not addressed to AMECHI or other occupants of the residence. Instead, the packages were addressed to other individuals such as “Ben Abbott” or “Ken Akeen.”

23. I know from my training and experience that victims often mail packages of cash, gift cards or other goods such as laptop computers or iPhones to addresses that they are directed to by the various online scammers. This investigation has also uncovered numerous victims who have mailed packages of cash, gift cards or iPhones after being directed by a person the victim believed was his or her online romantic interest.

24. I also know from my training and experience that sometimes fraudsters will sometimes direct victims to address the packages to nominees instead of the actual individuals who live at the address. Scammers and fraudsters sometimes take these actions to conceal the fact that the individuals living at the premises are the individuals receiving the packages. In my training and experience, individuals sometimes take these actions in an effort to avoid attracting law enforcement attention to the packages that they have received.

25. Earlier in this investigation, law enforcement obtained an email search warrant for AMECHI’s personal email account. During a review of that email search warrant return,

investigators discovered that AMECHI had emailed UPS regarding a package addressed to a “Ben” which is not AMECHI’s name or one of his known aliases. Similarly, on at least one occasion AMECHI called the Postal Service to pick up a package addressed to a “Ken Akeen,” another nominee.

26. Additionally, during the review of the return from the search of AMECHI’s email account, investigators uncovered multiple photographs of cash, iPhones and gift cards that are described more fully in Paragraph 51.

VICTIM¹ INFORMATION

Victim R.B.

27. Victim R.B. met a man on Instagram who she knew as Mason George (“Mason”) around December 2018. Victim R.B. communicated daily with Mason via text messages and WhatsApp. Mason told Victim R.B. he worked on an Exxon Mobile oil rig in the Gulf of Mexico. Around December 2018, Mason told her his oil rig crew was running out of food and Victim R.B. sent a wire transfer at Mason’s request.

28. Victim R.B. sent a wire transfer on August 28, 2019 for \$9,000 to Kenneth Ogudu at Chase Bank in Huntington, WV. This document reflects the purpose of the wire transfer was “personal loan.” Victim R.B. told investigators that Mason told her to tell her bank that was the purpose of the wire transfer. Victim R.B. stated that Mason called her on this date and advised he was on his way to Louisiana to see her when he was kidnapped by drug dealers in New Orleans. Mason told Victim R.B. that the drug dealers gave him the phone so he could call her and get the

¹ Investigators currently believe that the individuals labeled as victims in the next section are fraud victims. However, investigators may change their classification of these individuals if they learn more information which shows that one of the victims is more appropriately classified as a conspirator or a money mule.

ransom money. Mason asked Victim R.B. to wire \$9,000 to Kenneth Ogudu for his ransom. Victim R.B. stated this purpose of the wire transfer on the form was false but she did as Mason requested. Victim R.B. never met or communicated with Ogudu.

29. Victim R.B. wired \$3,000 to Ogudu's Chase Bank account on August 30, 2019. Victim R.B. also wired another \$10,000 to Ogudu on September 9, 2019. These wire transfer documents reflect the purpose of the wire transfers was "personal loan." Victim R.B. stated that Mason called her again and advised her the kidnappers wanted more money. Mason told her to wire another \$3,000.00 to Ogudu for the ransom. Victim R.B. admitted the stated purpose of the wire transfer on the bank form was false but she did as Mason directed.

30. Victim R.B. sent a wire transfer on September 9, 2019, for \$10,000 to Emeni at City National Bank in West Virginia from her account at Mid-South Bank. This document reflects the purpose of the wire transfer was for a "personal loan." Victim R.B. stated that Mason called her again on this date and advised her the kidnappers wanted even more money. Mason told her to send another \$10,000 to Emeni to pay the ransom. Victim R.B. stated this purpose of the wire transfer on the bank form was false but that Mason told her to tell her bank that was the purpose of the wire transfer. Victim R.B. never met or communicated with Kenneth Emeni.

31. Victim R.B. stated that Mason called her and advised he had been kidnapped by drug dealers again on his way to see her in Louisiana. Mason told her a man named Benjamin was going to come to her house to get the ransom. When Benjamin never showed up Mason called Victim R.B. again and asked her to wire \$12,000 to AMECHI for the ransom. On February 21, 2020, Victim R.B. wired AMECHI \$12,000.

Victim D.A.

32. In or around 2017, Victim D.A. met a person she knew as Richard Clem

(“Richard”) through Facebook. Victim D.A. lived in Nevada.

33. As part of the scheme to defraud, Richard and Victim D.A. communicated frequently via text messages, email and phone calls. As the result of Richard’s frequent communications, Victim D.A. falsely began to view Richard as a romantic interest and began what Victim D.A. was led to believe was a three-year online romance. After virtually dating Richard for a few months, Victim D.A. was fraudulently induced by Richard to repeatedly send money for his benefit based on a variety of false and fabricated reasons Richard provided to Victim D.A.

34. For example, Richard told Victim D.A. that he was a Lieutenant in the United States Army sent to Scotland on a peacekeeping mission. Richard also told Victim D.A. that he had a son who was injured in a car accident and that Richard needed money to pay his son’s hospitals bills.

35. Richard also told Victim D.A. that his platoon had discovered a gold mine and bought it from its previous owner. Richard then induced Victim D.A. to send him money to both pay the mine workers and to pay to ship the gold back to the United States. Richard promised Victim D.A. that he would share the gold with her when he returned to the United States.

36. Richard told Victim D.A. that he had been arrested in Scotland when he tried to leave the country because his visa had expired. Claiming falsely that he was leaving Scotland to travel to the United States to marry Victim D.A., Richard then induced Victim D.A. to send him more money so that he could renew his visa and return to the United States to marry her.

37. Richard also told Victim D.A. that he had been involved in a car accident and needed surgery to save his leg. Richard then induced Victim D.A. to send him a large amount of money to pay his falsely claimed medical bills.

38. Richard induced Victim D.A. to send funds to him multiple times and directed that the funds be sent to at least 15 different individuals. Richard never directed Victim D.A. to send the funds directly to him.

39. On or about March 2, 2020, Richard induced Victim D.A. to wire \$3,000 from her bank account held in Las Vegas, Nevada to AMECHI's bank account held in Huntington, Cabell County, West Virginia.

Victim B.F.

40. In or around January 2020, Victim B.F. met an individual she knew as Jerry Williams ("Jerry") online. Jerry frequently contacted Victim B.F. through Facebook and Google Hangouts. Victim B.F. resided in Indiana. Victim B.F. began to view Jerry as a romantic interest and began what she was led to believe was a virtual romance.

41. Jerry told Victim B.F. that his name was William James, but that he had to change it to James Williams and later to Jerry Williams for security reasons. Jerry also told Victim B.F. that he was a General in the United States Army stationed in Afghanistan. Jerry claimed that he wanted to leave the Army, come back to the United States, and marry Victim B.F. Jerry induced B.F. to send money for his benefit so that he (Jerry) could travel back to the United States.

42. Jerry induced Victim B.F. to send funds to him multiple times, through different individuals who he called his "security people," who were supposed to forward the funds to Jerry.

43. On or about April 28, 2020, Victim B.F. wired \$8,000 to defendant AUGUSTINE AMECHI's bank account held at PNC Bank. Jerry instructed Victim B.F. to write on the wire transfer form that the purpose of the wire was "paying off debt," which was false as Victim B.F. wired the funds at Jerry's direction and for his benefit and not to repay a debt.

44. On or about May 4, 2020, Jerry also fraudulently induced Victim B.F. to wire

another \$20,000 to defendant AUGUSTINE AMECHI's bank account held at PNC Bank. Jerry again instructed Victim B.F. to write on the wire transfer form that the purpose of the wire was "paying off debt," which was false, as Victim B.F. wired the funds at Jerry's direction and for his benefit and not to repay a debt.

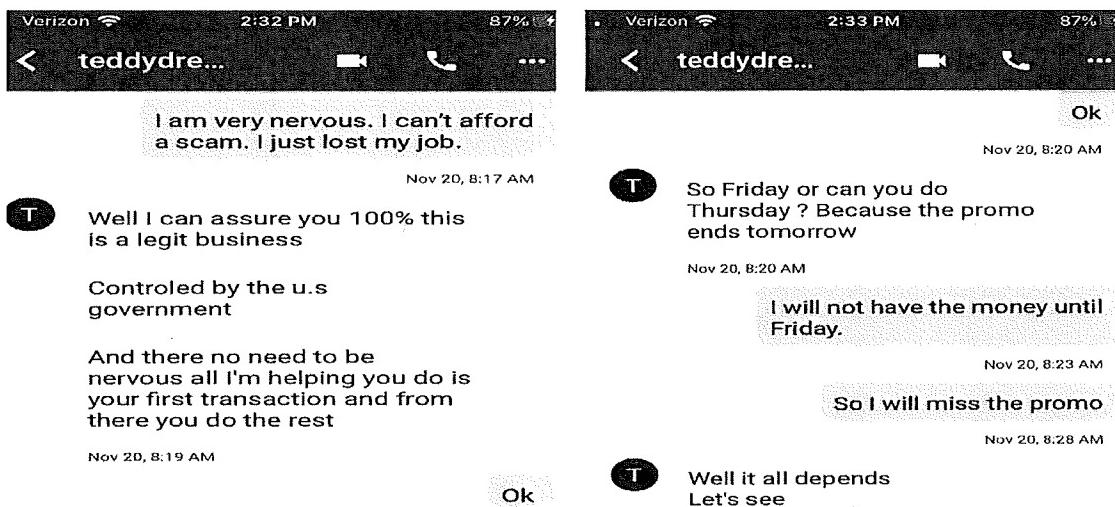
Victim J.F.

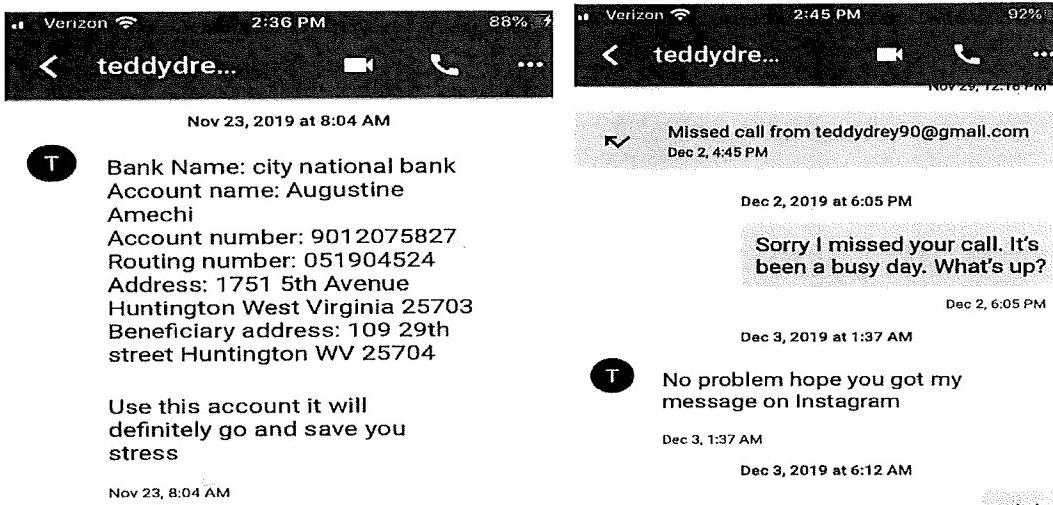
45. In or around the fall of 2019, an individual purporting to be Teddy Drey ("Teddy") contacted Victim J.F. online. Victim J.F. lived in Michigan. Teddy communicated with Victim J.F. through Instagram and the encrypted messaging application, "WhatsApp."

46. Teddy texted Victim J.F. that if Victim J.F. invested money in Bitcoin, his investment would double in 2-4 weeks.

47. Teddy induced Victim J.F. to wire \$1,000 to defendant AUGUSTINE AMECHI's City National Bank account located in Huntington, Cabell County, West Virginia. Teddy falsely assured Victim J.F. via text that this investment was not a scam.

Examples of text messages between Victim J.F. and Teddy





48. Victim J.F. never received any returns or profits from these Bitcoin “investments.”

FINANCIAL ANALYSIS

49. A review of AMECHI’s known bank accounts shows that he received wires or other deposits from at least 37 different individuals currently believed to be fraud victims from June 29, 2018 until May 29, 2019, which total to approximately \$108,601.00 at this time. However, as the financial breakdown below shows, AMECHI is believed to have received a much greater sum of fraud proceeds through cash deposits, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. AMECHI had reported wages totaling \$5,166.87 from 2017 through March 31, 2020. His reported taxable income is \$3,054 in 2018 and \$24,400 in 2019. AMECHI did not file taxes in 2017.

Deposits Received from Victims	\$108,601.00
Cash Deposits	\$105,718.03
Deposits from Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram	
Western Union, and Walmart	<u>\$159,983.03</u>
Total Illegal Proceeds Received by AMECHI	\$374,303.03

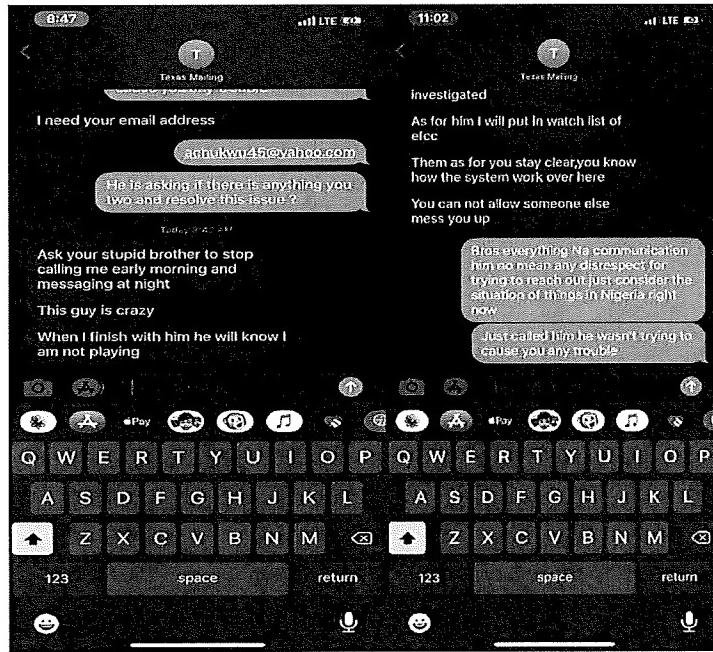
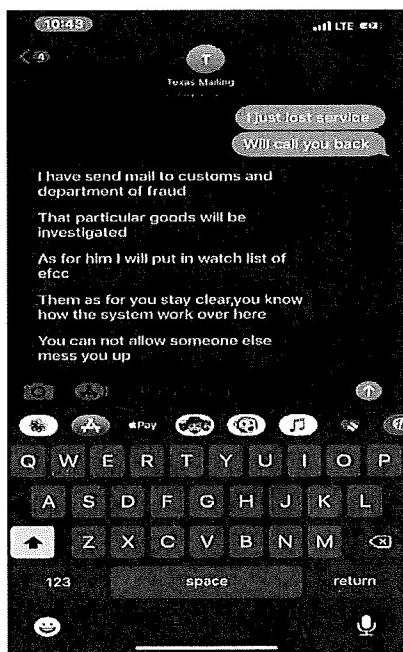
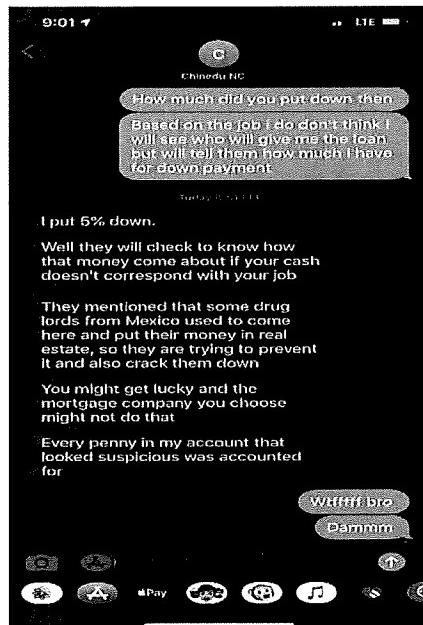
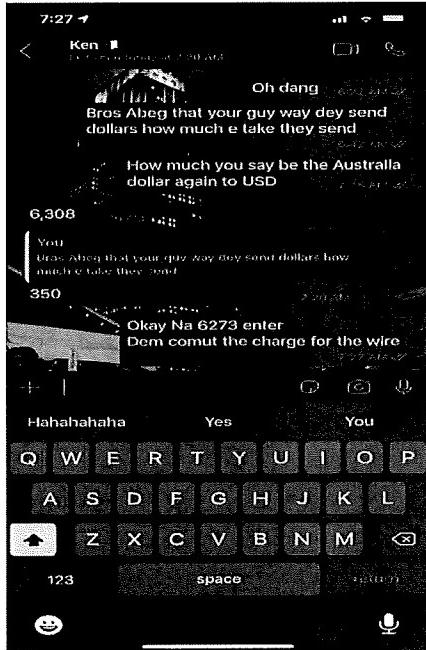
Example of Victim Funds Deposited in AMECHI's Bank Account

Date	Sender	Amount to AMECHI
11/29/19	Victim J.F.	\$1,000
2/21/2020	Victim R.B.	\$12,000
3/2/2020	Victim D.A.	\$3,000
4/28/2020	Victim B.F.	\$8,000
5/4/2020	Victim B.F.	\$20,000

INFORMATION LEARNED FROM EMAIL SEARCH WARRANTS

50. Law enforcement previously applied for and received numerous email search warrants. Investigators received information from several email accounts victims contacted during the fraud scheme as well as the Targets' email accounts, including one of AMECHI's email accounts. In their review of the information from AMECHI's email account, investigators learned that AMECHI used online banking and could access their bank information, including statements, deposit and transfer history electronically. AMECHI transferred a great deal of funds overseas and had records of those transfers sent to his email account as well.

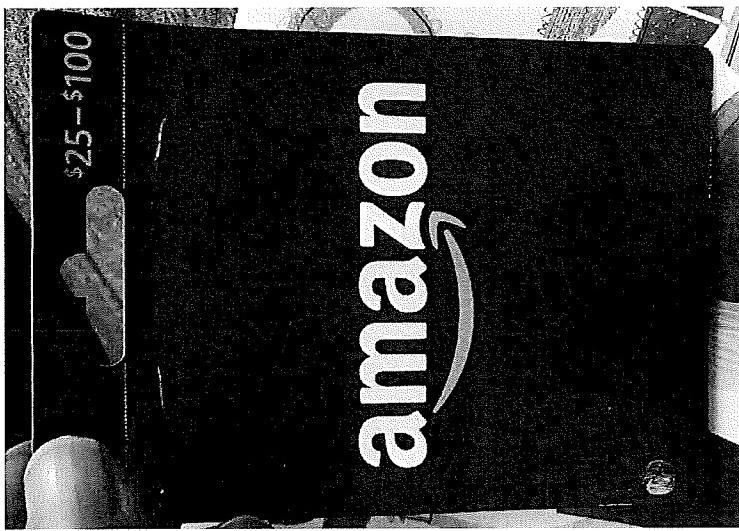
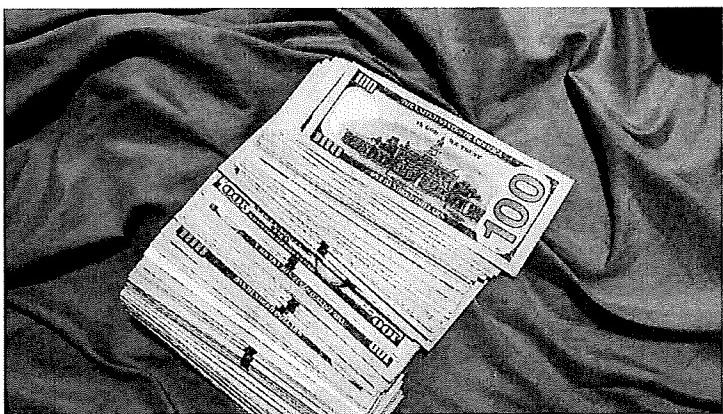
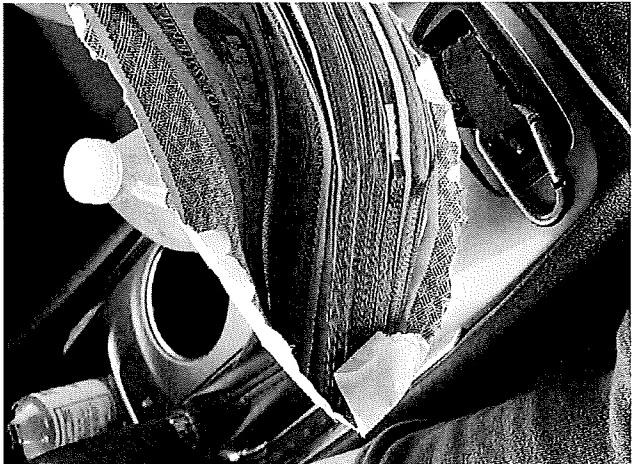
51. AMECHI sometimes texted with his associates as well and took screenshots of these texts which were uncovered from his email.

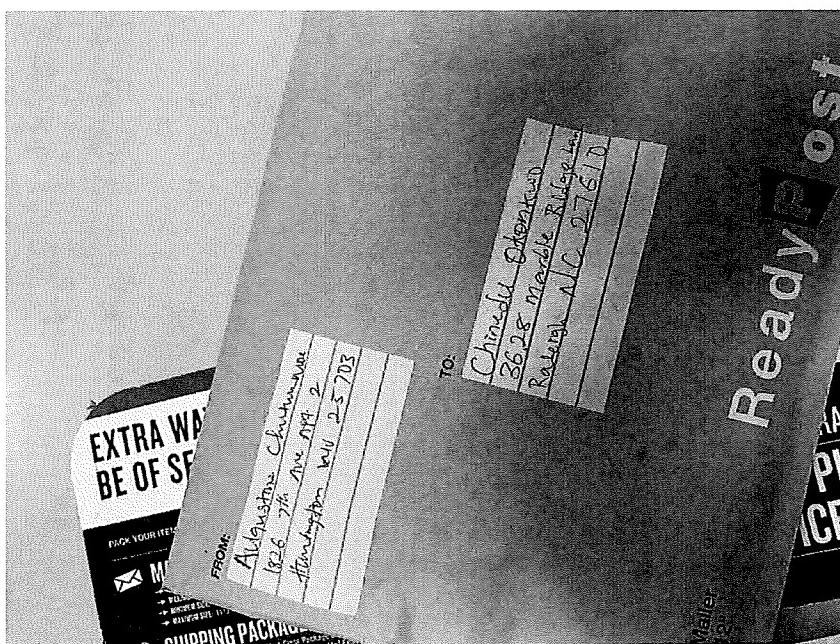
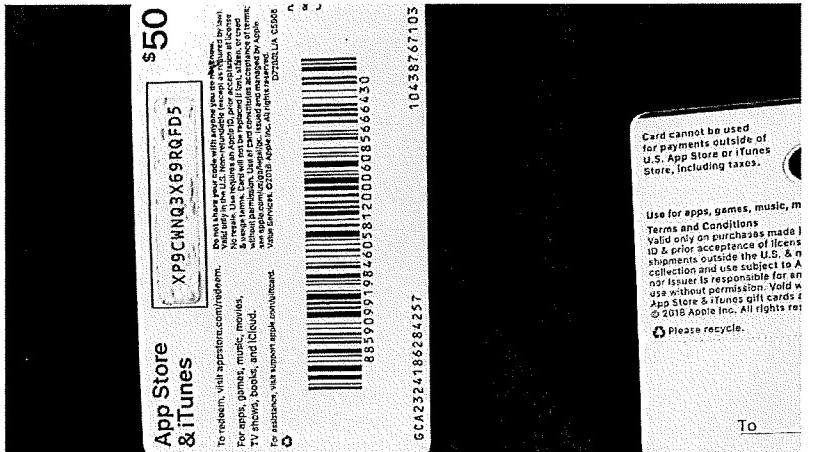


52. AMECHI often took pictures of the cash, gift cards, iPhones and packages that he received in the mail. AMECHI also took photographs of packages that he forwarded to individuals who are believed to be his associates in the fraud scheme. The last picture shown below shows

that AMECHI listed the SUBJECT PREMISES as his return address for when he sent a suspicious package to an individual who is believed to be one of his co-conspirators.







53. AMECHI's pictures of the cash, gift cards, iPhones, and packages that he received in the mail are particularly important because investigators learned that a number of packages were delivered to AMECHI's residence, the SUBJECT PREMISES, that were not addressed to AMECHI or any of the other known residents of the property. Instead the packages were addressed to the nominees listed below.

Examples of Suspicious Packages Delivered to the SUBJECT PREMISES

Date	Sender	Recipient
10/3/20	Glenda Cullum	Ken Akeen
10/22/20	A Hernandez	Tony Allen
11/2/20	Mrs. Hernandez	Tony Allen
11/2/20	Glenda Cullum	Ken Akeen
8/13/20	Diane Cantrell	Ben Abbott
9/16/20	Glenda Cullum	Ken Akeem
9/23/20	Glenda Cullum	Ken Akeem
2/12/21	Lisa Lockhart	Junior Vic

54. The packages may have been sent from fraud victims. The email search warrant return also revealed that AMECHI used the email account that has been connected to him achukwu45@yahoo.com, to write to UPS about a missing package addressed to a “Ben.” Similarly, AMECHI’s email account had multiple screenshots that showed he had been tracking the delivery of packages. Below are two screenshots from AMECHI’s account related to the delivery of packages addressed to a “Ben.”

Next Steps for Your Missing UPS Package

donotreply@ups.com
To achukwu45@yahoo.com
Today at 1:26 PM

Dear Ben,

Thank you for contacting us about your missing shipment. A representative from your local package center will call you within one hour with an update.

Our goal is to determine if our driver can provide additional guidance to help find your package(s). We will share any applicable information with you soon. However, a package investigation will be required if our driver is unable to provide additional information.

If an investigation is required, we recommend that you contact the company or person who sent you the shipment. This is helpful for the following reasons:

- The shipper has all of the information we need to investigate
- The shipper can possibly send a replacement shipment
- Most shippers want to know if their customers are having trouble with an order, and some shippers have additional resolution options

However, if you prefer to report a missing or lost package yourself,

Tracking Details

1Z3F19X30291295272

From: WAIKOLOA, HI, US

Delivered

Delivered On: 08/17/2020
12:35 PM

Received by: BEN

Location: Residential

Service Level: UPS 2nd Day Air®

Weight: 0.10 LBS

Want to know when?

Get FREE estimated delivery windows on most UPS packages.

Continue

Package Progress

HUNTINGTON, WV, US	08/17/2020 12:35 PM	DELIVERED
Huntington, WV, US	08/17/2020 9:10 AM	Out For Delivery Today
Huntington, WV, US	08/17/2020 5:20 AM	Loaded on Delivery Vehicle

55. Similarly, investigators learned that there was a package scheduled to be delivered to a “Ken Akeen” on or around December 23, 2020. The Postal Service was originally unable to deliver the package and left a note that the package was available for pickup. An individual calling from the phone number 304-688-1205² called the Postal Service about the package and identified himself as Ken Akeen. The postal employee informed the caller that he would have to show his ID if he wanted to pick up the package from the post office. After the caller learned this information the caller then stated that Ken was not available but actually traveling abroad.

56. In my training and experience, AMECHI’s actions described in the above two paragraphs show that he was expecting these packages and intended them to be delivered to him.

² Mark Noe was the subscriber to the 304-688-1205 number. However, Mark Noe is the AMECHI’s relative the investigation has revealed that AMECHI is the user the 304-688-1205 number as he has listed this number as his own with several financial institutions and businesses.

AFFIANT BACKGROUND IN FINANCIAL CRIMES INVESTIGATIONS

57. As a Special Agent with the Secret Service, your Affiant has had training and experience in financial crimes investigations. Based upon my training, experience, and knowledge, I am aware of the following:

- a. Monetary instruments, such as checkbooks, money orders, and cashier's checks, utilized by individuals engaged in illegal activities such as financial fraud schemes are oftentimes secured in safe-deposits, locked drawers, and lock boxes.
- b. In these types of online fraud schemes, victims often mail packages to the perpetrators of the fraud. The packages can have cash, various gift cards and even iPhones, laptop computers or watches inside.
- c. Individuals involved in other illegal activities oftentimes place income and assets in the name of nominees, in hopes of shifting the responsibility for the payment of tax and concealing their ownership to protect the assets from seizure. However, it is also my experience that the titles and deeds to said assets are maintained by the subject and not the nominee owner.
- d. Business entities generally require that specific business and personal financial records be maintained for use in applying for loans at financial institutions, for tax preparation, and for audit purposes. These records are commonly stored for lengthy periods of time at residences, at business offices, in vehicles and other storage facilities.
- e. Records can be stored in paper format or in digital form. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer - can store thousands of documents. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person and can store digital copies of records. Smartphones and other smart electronic devices also often have access to online banking accounts through mobile applications or web browsers. These accounts are often utilized to maintain the business records of expenses and income.
- f. The Internet affords individuals several different venues for obtaining, completing, and storing business records.
 - i. Individuals also use online resources to retrieve and store records. Some online services allow a user to set up an account with a

- remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of records may be found on the user’s computer, smartphone, or external media in some cases.
- ii. A digital technology related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to engage in banking activity, money transfers, bill payments, and engage in other financial related activities.
 - g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for purposes of maintaining records. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
 - h. Paper copies, or hard copies, of business and personal financial records can also be stored in file cabinets, desk drawers, cabinets, safes and safe-deposit boxes, lock boxes, wallets, purses and handbags, garbage bags, cardboard boxes, and other storage containers large enough for paper retention.
 - i. Individuals engaged in conspiracies to commit other crimes often communicate with one another as well as with unwitting accomplices. These communications can occur in many forms including person to person, telephonic, text messages and electronic such as email. These communications typically involve details pertaining to the scheme, directions to subordinates as to how to carry out certain elements of the scheme and correspondence to and from unwitting third parties such as financial institutions, investors, and accountants.
 - j. Individuals involved in criminal endeavors conduct financial transactions in a manner to avoid law enforcement detection. These individuals exchange currency for various types of monetary instruments including postal money

orders, cryptocurrencies, and bank cashiers' checks and, thereby, attempt to disguise and conceal their true business and personal affairs.

k. To accurately reconstruct the personal financial histories of persons, all forms of personal records reflective of financial transactions are required.

58. Your Affiant has no reason to believe that the search is likely to result in the seizure of any drafts of publications (such as books, newsletters, website postings, etc.) that are unrelated to the search and stored on the target computers. Thus, the search will not implicate the Privacy Protection Act, 42 U.S.C. § 2000aa. I have no reason to believe that the search is likely to result in the seizure of a mail server. Thus, the search will not implicate the Electronic Communications Privacy Act, 18 U.S.C. § 2701.

59. Your Affiant believes that given the continuing nature of financial crimes, as well as the length of the scheme, there is probable cause to believe that evidence of violations of federal law, including, but not limited to, 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); and 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity), will be present in the SUBJECT PREMISES as described in Attachment B, and on the person of AMECHI as described in Attachment A, when the search is conducted. Thus, even if AMECHI uses an electronic device (such as a laptop or a mobile smart phone) to access the Internet and digital records, his own financial records, there is probable cause that evidence of this access will be found in the SUBJECT PREMISES in addition to being on each of their individual persons and devices seized.

BACKGROUND ON SEIZURE AND SEARCH PROCEDURES FOR ELECTRONIC DEVICES AND DIGITAL EVIDENCE IN RELATION TO FRAUD INVESTIGATIONS

60. As described further in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other

storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B), of any device belonging to or used by AMECHI or where ownership cannot be determined.

61. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

- a. AMECHI and his associates used cellphones, computers, and other electronic devices to communicate with the victims during the fraud scheme. At least one of the victims were defrauded by Bitcoin scams as he sent money to purchase Bitcoin but never received the cryptocurrency. Bitcoin is held virtually and evidence of fraudulent Bitcoin transfers would also most likely be digital.
- b. The information gathered from the email search warrants shows that AMECHI used electronic devices to carry out these frauds, whether by making financial transfers or sending banking information or pictures of cash, iPhones and gift cards to his associates.
- c. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- d. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- e. Wholly apart from user-generated files, computer storage media, in particular, computers’ internal hard drives, contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

- f. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

62. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about when the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account

session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Lastly, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. I know that when an individual uses a computer to complete illegal financial activities, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of

Internet discussions about the crime; and other records that indicate the nature of the offense.

63. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

64. Additionally, based upon my training and experience and information related to

me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime — including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

65. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. The process by which the search and seizure of such computers or other electronic devices will occur in this instance is more formally laid out in Attachment B.

BIOMETRIC ACCESS TO DEVICES

66. This warrant permits law enforcement to compel AMECHI to unlock any electronic devices (“DEVICES”) or computers requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follow:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.
- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for eight hours *and* the passcode or password has not been entered in the last six days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.
- h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of AMECHI to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of AMECHI and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of AMECHI and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel AMECHI state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel AMECHI, to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that

may be used to unlock or access the DEVICES.

PROBABLE CAUSE SUMMARY

67. Based on the victim interviews and financial records, there is probable cause to believe that AMECHI is involved in a fraud scheme which regularly used email, text messaging and other electronic and Internet based methods of communication as well as money transfers. As stated earlier in the Affidavit, AMECHI has been charged by a federal Grand Jury as detailed in 3:21-cr-00069. AMECHI is facing multiple fraud charges alleging violations of 18 U.S.C. 18 U.S.C. § 1343, 18 U.S.C. § 1957 and 18 U.S.C. § 2315.

68. Based upon the foregoing, I submit that there is probable cause to believe that AMECHI and the other Targets have committed the Target Offenses, and that AMECHI has used a cellular telephone and other electronic devices in furtherance of the Target Offenses. For example, as described above, as part of the fraud scheme, the Targets and their associates would contact victims through email, text messages or online dating and social media websites. The email search warrant returns also revealed that AMECHI communicated with the Targets and other associates through text. Additionally, evidence obtained from AMECHI's email account revealed that AMECHI used online banking, email and text messages (particularly pictures messages) and other electronic and Internet based methods of communication in order to obtain bank account information and conduct money transfers in furtherance of the scheme.

69. Law enforcement observed AMECHI at the SUBJECT PREMISES on May 24, 2021. Financial records obtained during the investigation also revealed that AMECHI has resided at the SUBJECT PREMISES during the fraud scheme. Upon information and belief, people generally keep their personal cellular phones, computers and other devices at their homes.

70. Based on the foregoing, I further submit that there is probable cause to believe that AMECHI is currently residing at the SUBJECT PREMISES and that one or more of AMECHI's electronic devices—including AMECHI's cell phone—will be found inside the Subject Premises, and that said devices are likely to contain evidence of the Target Offenses. As such, this affidavit seeks authorization to search the SUBJECT PREMISES, and to seize and subsequently search any cellular telephones and computers belonging to AMECHI.

CONCLUSION

71. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

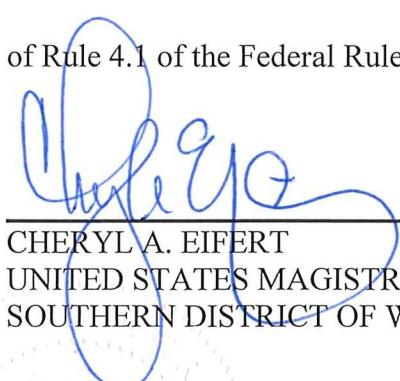
72. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,



TERRY HEDRICK
SPECIAL AGENT
UNITED STATES SECRET SERVICE

Subscribed and sworn-to by the Affiant telephonically in accordance with the procedures of Rule 4.1 of the Federal Rules of Criminal Procedure, on May 25, 2021.



CHERYL A. EIFERT
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA